



במה כרוך ניהול בחברות טכנולוגיות בהתחשב באתגרי הסייבר הרבים העומדים לפתחנו? קורס מנהלי סייבר בטכניון מציע סט כלים מתקדם ומגוון מאין כמוהו ללמידת התחום על בורי

אתגרים חדשים בניהול טכנולוגי בעידן הסייבר

לאחרונה, אנו חשופים לגל אדיר של מתקפות סייבר, ונדמה כי הן מאיימות עלינו מכל הכיוונים. רק בשבוע שעבר התבשרנו על מתקפה שחשפה מומחה מחשבים מעזה שפרץ והאזין לתשדורת של כלי טייס צבאיים. בכל פעם נשמעת אותה טענה שהמתקפה האחרונה, "תפסה" את הארגון לא מוכן, ושלא הוכן "מדריך הפעלה" כיצד לנהוג במקרה של מתקפת סייבר.

שאל אמיר, איש סייבר ותיק ומנהל אקדמי בתכנית החדשה למנהלי סייבר בטכניון לימודי המשך, מבהיר מספר נקודות על תפקידו של המנהל בהתמודדות עם אתגרי הסייבר - האם תחום הסייבר בארגון הינה בתחום אחריותו של איש ה-IT ושלו בלבד או גם של המנהלים הבכירים בארגון? (אחד האתגרים בתחום הינו שמנהלי ה-IT רואים את תחום הסייבר כאבטחת מידע בלבד).

ניתוח סיכוני הסייבר בארגון

תחום הסייבר דורש מהמנהל יכולות טכנולוגיות בתחומים שונים ורבים מצד אחד ויכולות עסקיות והבנה של תהליכים עסקיים מהצד השני. יכולות טכנולוגיות במגוון תחומים כוללת שלל נושאים ובעיקר את:

- **תחום התקשורת** - הרשת הפנים ארגונית, הרשת הארגונית וירטואלית והרשת האינטרנטית
- **מסדי נתונים** - כולל Big Data, Data warehouse וכן עיבוד, חיפוש והפקת המידע המתאים
- **מרחב האינטרנט** - אתרים, אפליקציות, שירותים ויישומי ענן - Cloud
- **האינטרנט של הדברים** - IOT - עולם החפצים והביטחון האישי-ארגוני HLS הבנה עסקית בתחום כוללת בעיקר את היכולת לנתח את משמעותיות איומי הסייבר מבחינת הערכות סיכונים ונזקים, השפעות כלכליות ואומדן ערך כלכלי להגנת סייבר, ומאלו נגזרות החלטות כמה, כיצד

האם זה מספק? האם בכך אנו מוכנים לתרחיש של התקפה הבאה? האם חוסר הידע המקצועי של המנהלים בדרכים השונים בארגון וההסתמכות על חוות הדעת המקצועית של אנשי ה-IT יכולים לספק "שקט תפעולי" לארגון? האם המנהל האחראי על שכבות הארגון מקבל מספיק מידע ושואל את השאלות הרלוונטיות על מנת להדגיש את אסטרטגיית האבטחה הנכונה?

התפקיד הניהולי מחייב מעורבות, מחויבות וכניסה לפרטים-המנהל האחראי צריך לשאול את השאלות הנכונות, להיכנס לפרטים טכניים עד כדי בחינת הקוד המפותח, בחינת התפקוד והאינטגרציה של המרכיבים השונים במערכת על מנת לוודא שהאסטרטגיה שנקבעה מיושמת הלכה למעשה.

למעשה כל יצרן דורש את הידע הבסיסי ואת מגוון ההסמכות הנדרשות להפעלת הציוד בצורה יעילה ונכונה. כתוצאה מכך ארגונים משמרים את מיטב המומחים של אותם יצרנים בעלויות כוח-אדם גבוהות. מנהל הארגון צריך לבחון את כלל מחזור החיים של הטיפול באתגרי הסייבר, ולא להסתכל על הדברים רק בהיבט של שימור מומחים לתחום טכנולוגי או כלי מסוים. בנוסף, צריך המנהל לבחון אם הארגון בעל כושר מלא לכל תרחיש, והאם כל מגוון התחומים (Domains) מטופלים באופן מקצועי - כלומר, לתכנן אסטרטגית ולהתוות מדיניות השקעה ודרכי פעולה על מנת למקסם את ביטחון של הארגון בכפוף לתקציב מוגבל.

למה צריכים מנהלי סייבר בארגונים?

בלימודי ניהול, תחום הסייבר הוא בעל משמעות שונות ואחרות, בהשוואה ללימודי ניהול ביתר המקצועות והתחומים במשק. מנהלים מתמקדים בדרך כלל בתחום הניהולי הקלאסי של תכנון פרויקטים, תכנון ובקרה ניהולית, הנעת עובדים ותמרוץ עובדים.

מנהל מערך הסייבר בארגון צריך להיות בעל ידע נרחב בכל אחד מהתחומים שהוזכרו בכדי לקבל החלטות ולבצע את המטלות הניהוליות בארגון, במגוון הרבדים השונים שתחום הסייבר

דורש, ובעיקר עליו לדעת כיצד להקים את מערך ההגנה על נכסי הארגון, הידע והמשך התפקוד השוטף של הארגון (הן ארגון ייצור והן ארגון שירות) - מתודולוגיית הגנה ותפעול המערכות הארגוניות.

מה המשמעות של הכנסת אמצעים ותוכנות חדשות לארגון?
הכנסת אמצעים ותוכנות חדשות לארגון משמע כל מחזור החיים בניהול מבחינת הדרישה (הצורך), בחינת אלטרנטיבות וחקר ביצועים, משמעותיות מבחינת עלויות (קנייה, פיתוח, תחזוקה, קבועות, משתנות), אופן קבלת החלטות והגורמים המשתתפים (בעלי העניין), רכש, פיתוח, ביצוע בדיקות קבלה, כולל מבדקי חדירה והמשך טיפול תחזוקה שוטפת, ניהול גרסאות ושיפורים. מתודולוגיית לפיתוח תוכנה (בארגון אשר ייעודו



קמפוס הטכניון במתחם שרונה תל אביב

ואיפה להשקיע ולכן להפנות את מאמצי כוח האדם והתקציב.

כאמור, מתקפת סייבר עלולה לשתק ולפגוע בכל שכבות הארגון. היא עלולה להוות משבר באמון הנרכש לאורך זמן בין ההנהלה והעובדים, והחשוב ביותר - האמון שנבנה לאורך שנים רבות בין הלקוחות לארגון. מתקפת הסייבר עלולה גם לחשוף מידע מאוד רגיש עד כדי נטישת לקוחות.

רוב המשאבים למידור ולהגנה מפני התקפות סייבר יופנו לרכישת ה-Firewall הטוב ביותר בשוק, או את תכונת ההגנה החזקה החדשה שהושקה בגרסת התוכנה החדשה, וזאת בעיקר מחוסר הידע הטכנולוגי והניהולי שהוצג לעיל.

לפתח תוכנה/מוצרים) והדרך שבה ניתן ליישם את משמעותיות הסייבר.

קורס מנהלי סייבר בטכניון

המחשה הקרובה לתיאור האתגרים הרבים הקיימים בתחום היא משחק שח, כאשר השחקן מתמודד מול יריב ללא אפשרות לראות את כלי היריב וללא ידיעה ברורה מהן המטרות של היריב. השחקן מכיר את היכולות של כל כלי וכלי (כל כלי בלוח השח הוא בעל יכולות אחרות) ויכול להחליט עם איזה כלי לבצע מהלך מסוים.

ובחזרה לתחום הסייבר - כל כלי מייצג תוכנה (המונח המקצועי בסייבר או בתוכנה הינו "כלי" או Tool Utility) ומנהל הסייבר צריך לקבל החלטה איזה כלי כדאי לרכוש לארגון, מה היכולות של כל כלי ומה מידת הכושר שלו, כיצד לפקח ומתי להשתמש בכלים, אילו כלים חסרים, מה כדאי לפתח וכמובן כיצד מביאים לידי ביטוי ועצמה את השימוש בכל האמצעים יחד.

קורס למנהלי סייבר בטכניון כולל התעמקות בכל הנושאים והכלים, הן הטכנולוגיים והן העסקיים, ואינו מסתפק בסממאות והגדרות. רק לשם המחשה, בתחום התקשורת הקורס כולל את המשמעות של כל פרוטוקולי התקשורת החשובים כמו למשל (רשימה חלקית): TCP/IP, UDP, SMTP, SNTP, FTP, DNS, RIP, ARP, ICMP, תוך שילובם והבנת כלי ניטור רשת וכלים לחומת אש (Firewall).

מעבר לתחום הנלמד של DB, BI כולל הקורס את מגוון כלי ההגנה של הסייבר, המבוססים על יכולת עיבוד מגוון ומסות של נתונים, כמו כלי SIEM, ARC sight, MacAfee ועוד. בתחום של מתודולוגיות כולל הקורס את המגוון וההתאמה לסייבר מבחינת תקנים ISO 27001 ו-SPSMM, משמעות תכנון תוכנת הגנה, בחירת כלים ועוד.

למידע נוסף והזמנה למפגש מידע, ניתן ליצור קשר עם ברקת פלד בטל. 03-6966662 שלוחה 5



*כותב המאמר - **שאל אמיר**, מנהל אקדמי של תכניות הסייבר בטכניון - היחידה ללימודי המשך ולימודי חוץ, קמפוס שרונה ת"א.

בעל ניסיון של יותר מ-20 שנה במגזר הביטחוני בפיתוח מערכות שליטה ובקרה, מערכות זמן אמת ופיתוח סימולטורים - בדגש על תחומי הפיתוח למגוון יכולות הסייבר בתקיפה והגנה. משמש כיום כמנהל המדעי-טכנולוגי של סימולטור הסייבר באוניברסיטת אריאל. בעל תואר ראשון BSC מהטכניון ו-MSc במערכות מידע מאוניברסיטת ת"א.